

Bruno Dutertre / Bettina Könighofer (Eds.)

PROCEEDINGS OF THE 26TH CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2026



Bruno Dutertre / Bettina Könighofer (Eds.)

PROCEEDINGS OF THE 26TH CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED
DESIGN – FMCAD 2026

Conference Series: Formal Methods in Computer-Aided Design

Volume 7

Conference Series: Formal Methods in Computer-Aided Design

Series edited by:

Warren A. Hunt, Jr., The University of Texas at Austin
Austin, TX 78705 | hunt@cs.utexas.edu

Georg Weissenbacher, TU Wien
Karlsplatz 13, 1040 Vienna, Austria | georg.weissenbacher@tuwien.ac.at

The Conference on Formal Methods in Computer-Aided Design (FMCAD) is an annual conference on the theory and applications of formal methods in hardware and system verification. FMCAD provides a leading forum to researchers in academia and industry for presenting and discussing groundbreaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems. FMCAD covers formal aspects of computer-aided system design including verification, specification, synthesis, and testing.

Information on this publication series and the volumes published therein is available at www.tuwien.ac.at/academicpress.

Volume 7 edited by:

Bruno Dutertre, Amazon Web Services
2795 Augustine Drive, Santa Clara, CA 95054, USA | dutebrun@amazon.com

Bettina Könighofer, TU Graz
Rechbauerstraße 12, 8010 Graz, Austria | bettina.koenighofer@tugraz.at

Bruno Dutertre / Bettina Könighofer (Eds.)

PROCEEDINGS OF THE 26TH CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2026

Cite as:

Dutertre, B., & Könighofer, B. (Eds.). (2026). *Proceedings of the 26th Conference on Formal Methods in Computer-Aided Design – FMCAD 2026*. TU Wien Academic Press. <https://doi.org/10.34727/2026/isbn.978-3-85448-093-8>

TU Wien Academic Press, 2026

c/o TU Wien Bibliothek
TU Wien
Resselgasse 4, 1040 Wien
academicpress@tuwien.ac.at
www.tuwien.at/academicpress



This work is licensed under a Creative Commons attribution 4.0 international license (CC BY 4.0).
<https://creativecommons.org/licenses/by/4.0/>

ISBN (online): 978-3-85448-093-8
ISSN (online): 2708-7824

Available online: <https://doi.org/10.34727/2026/isbn.978-3-85448-093-8>

Media proprietor: TU Wien, Karlsplatz 13, 1040 Wien
Publisher: TU Wien Academic Press
Publication series editor: Warren A. Hunt, Jr. and Georg Weissenbacher
Editors (responsible for the content): Bruno Dutertre and Bettina Könighofer

Preface

These are the proceedings of the twenty-sixth International Conference on Formal Methods in Computer-Aided Design (FMCAD), held in Graz, Austria, from September 14–18, 2026.

FMCAD was first organized in 1996 and was held biennially until 2006, when it merged with the CHARME conference to become a single annual event. Since then, FMCAD has been held every year at venues around the world. Thus, FMCAD 2026 also marks thirty years since the first edition of the conference.

FMCAD 2026 continues the conference’s tradition of covering formal aspects of computer-aided system design, including verification, specification, synthesis, and testing. It serves as a leading forum for researchers from academia and industry to present and discuss new methods, technologies, theoretical results, and tools for formal reasoning about computing systems. Reflecting the growing interaction between formal methods and artificial intelligence, this year’s call for papers was extended to explicitly include two additional areas. The first concerns formal verification of data-driven AI systems, addressing challenges such as safety, robustness to adversarial inputs, reliability, fairness, and compliance with regulatory requirements. The second concerns applications of AI to enhance formal methods techniques, including invariant and specification inference, learning-based heuristics for verification and synthesis, and data-driven verification workflows. By explicitly incorporating these topics into the scope of FMCAD, we aim to encourage contributions at the rapidly developing intersection of formal reasoning and AI.

The conference was hosted by Graz University of Technology (TU Graz) and was co-located with the 18th International Conference on Verified Software: Theories, Tools and Experiments (VSTTE 2026). VSTTE took place on September 14, followed by a joint VSTTE/FMCAD tutorial day on September 15. The main FMCAD conference was held from September 16–18.

The joint VSTTE/FMCAD tutorial day featured three tutorials:

- The VSTTE tutorials:
 - *A Tutorial on Algebraic Verification of Arithmetic Circuits: Gröbner Bases in Practice*, by Daniela Kaufmann
 - *Verification of DNNs with Marabou*, by Omri Isac
- The FMCAD tutorial:
 - *Verifying Rust code with Verus*, by Travis Hance

The main FMCAD conference featured three invited talks:

- *CSLib: Building a Platform for AI-assisted Formal Verification in Lean*, by Clark Barrett
- *The Parable of the Square-Dancing Witches and Wizards*, by Claire Xenia Wolf
- *The Vampire Diary*, by Laura Kovács

FMCAD 2026 received 224 submissions, a substantially higher number than in a typical year. We are both delighted and proud to see such strong interest in the conference, which reflects the vitality of the FMCAD community and the continued relevance of formal methods across a broad range of research areas. Following the rebuttal phase, 172 papers remained under consideration, of which the program committee selected 70 papers for publication, corresponding to an overall acceptance rate of 31.25%. Each submission underwent a rigorous peer-review process and received at least three reviews; the large majority of the papers received four reviews. Among the accepted papers, 46 are regular papers (39 long and 8 short), and 24 are tool or case study papers (18 long and 6 short). For the second year, FMCAD introduced voluntary artifact evaluation. The artifacts were assessed by selected members of the program committee. A total of 107 artifacts were submitted and 48 of the accepted papers included artifacts.

The accepted papers span a broad range of topics in formal methods, including SAT and SMT solving, program verification and synthesis, hardware verification, neural-network verification, machine-learning-assisted reasoning, runtime monitoring and specification learning, model checking, proof generation, security and privacy, probabilistic verification, and parallel solving techniques. The breadth of these contributions reflects both the continued development of foundational formal-methods techniques and their expanding application to emerging areas of computing.

FMCAD 2026 also continued the annual FMCAD Student Forum, which has been held since 2013. The forum provides a platform for students to present ongoing research to the wider formal-methods community, receive feedback, and engage with researchers from academia and industry. The FMCAD Student Forum 2026 was organized by Tanja Schindler and Lee Barnett and featured short presentations and posters for 18 accepted contributions.

The conference proceedings are published as Open Access by TU Wien Academic Press and are also made available through the IEEE Xplore Digital Library.

FMCAD 2026 was made possible through the support and efforts of many individuals and organizations. We would like to thank Georg Weissenbacher for serving as publication chair and for his continued support in preparing the conference proceedings. We thank Martin Tappler, our publicity chair, and Stefan Pranger, our web chair, for their work in promoting the conference and maintaining the conference website. We are grateful to Tanja Schindler and Lee Barnett for organizing the Student Forum. We also sincerely thank Ursula Urwanisch, Martina Piewald, and Julia Siebenhofer for their work in organizing the conference in Graz and for expertly managing the numerous logistical and practical aspects of the event. We are grateful to Graz University of Technology for hosting FMCAD 2026 and to everyone who contributed to making the conference possible.

We sincerely thank all of the members of the program committee for the substantial time and expertise they dedicated to the review process. Their efforts were essential not only for assembling a strong technical program, but also for providing authors with constructive feedback to improve their work. As the unexpectedly large number of submissions created a considerable additional reviewing workload, we are especially grateful to the program committee members who joined the committee at short notice to help us manage this increase. Their willingness to contribute their time and expertise on very short notice was invaluable in maintaining the thoroughness and quality of the review process.

We are grateful to our sponsors for their generous support and gratefully acknowledge the contributions of the following organizations, listed in alphabetical order: Amazon Web Services (AWS), Cadence Design Systems Inc., TTTECH, TU Graz, and TU Wien.

We sincerely thank everyone who submitted or presented a paper, gave an invited talk, contributed a tutorial, participated in the Student Forum, or otherwise helped shape the program. Finally, we thank all attendees of FMCAD 2026 for supporting the conference and for making FMCAD an engaging and enjoyable event.

September 2026

Bettina Könighofer	TU Graz, Austria
Bruno Dutertre	AWS, USA

Organizing Committee

Program Co-Chairs

Bruno Dutertre
Bettina Könighofer

Amazon Web Services, USA
Graz University of Technology, Austria

Student Forum Chairs

Tanja Schindler
Lee A. Barnett

University of Basel, Switzerland
Amazon Web Services, USA

Publicity Chair

Martin Tappler

TU Wien, Austria

Web Chair

Stefan Pranger
Thomas Hader

Graz University of Technology, Austria
TU Wien, Austria

Publication Chair

Georg Weissenbacher

TU Wien, Austria

FMCAD Steering Committee

Clark Barrett
Armin Biere
Ruzica Piskac
Anna Slobodova
Georg Weissenbacher

Stanford University, CA, USA
University of Freiburg, Germany
Yale University, CT, USA
Arm, TX, USA
TU Wien, Austria

Board of the FMCAD Association

Armin Biere
Roderick Bloem
Georg Weissenbacher
Florian Zuleger

University of Freiburg, Germany
Graz University of Technology, Austria
TU Wien, Austria
TU Munich, Germany

Program Committee

FMCAD 2026 Program Committees

Bruno Dutertre (co-chair)	Amazon Web Services, USA
Bettina Könighofer (co-chair)	Graz University of Technology, Austria
Erika Abraham	RWTH Aachen University
Bernhard Aichernig	Graz University of Technology
S. Akshay	IIT Bombay
Guy Amir	Cornell University
Timos Antonopoulos	Yale University
Guy Avni	Department of Computer Science, University of Haifa
Thom Badings	University of Oxford
Kyungmin Bae	Pohang University of Science and Technology (POSTECH)
Kshitij Bansal	Google
Dirk Beyer	LMU Munich, Germany
Armin Biere	University of Freiburg
Per Bjesse	Synopsys Inc.
Nikolaj Bjørner	Microsoft
Martin Blicha	University of Lugano
Roderick Bloem	Graz University of Technology
Gianluca Bonifazi	Università Politecnica delle Marche
Shaowei Cai	Institute of Software, Chinese Academy of Sciences
Francesca Cairoli	University of Trieste
Mauricio Castillo-Effen	Lockheed Martin Advanced Technology Laboratories
Pablo Castro	Universidad Nacional de Rio Cuarto, Argentina
Rohit Chadha	University of Missouri
Chih-Hong Cheng	Chalmers University of Technology
Alessandro Cimatti	Fondazione Bruno Kessler
Thao Dang	CNRS/VERIMAG
Yuxin Deng	Shanghai University of Finance and Economics
Luca Di Stefano	TU Wien
Rayna Dimitrova	CISPA Helmholtz Center for Information Security
Marco Eilers	ETH Zurich
Yizhak Elboher	The Hebrew University of Jerusalem, Israel
Constantin Enea	Ecole Polytechnique
Marco Faella	Università di Napoli "Federico II"
Katalin Fazekas	TU Wien
Grigory Fedyukovich	Florida State University
Pascal Fontaine	Université de Liège, Belgium
Hadar Frenkel	Bar-Ilan University
Martin Fränzle	Carl von Ossietzky Universität Oldenburg
Mirco Giacobbe	University of Birmingham
Nicola Gigante	Free University of Bozen-Bolzano, Italy
Alberto Griggio	Fondazione Bruno Kessler
Shibashis Guha	Tata Institute of Fundamental Research

Liana Hadarean	Amazon Web Services
Osman Hasan	National University of Sciences and Technology (NUST)
Paula Herber	University of Münster
Marijn Heule	Carnegie Mellon University
Lukáš Holík	Brno University of Technology
Antti Hyvärinen	Certora
Alexey Ignatiev	Monash University
Radoslav Ivanov	RPI
Mikoláš Janota	Czech Technical University in Prague
Nils Jansen	Ruhr University Bochum
Susmit Jha	SRI International
Martin Jonáš	Masaryk University, Czechia
Daniela Kaufmann	TU Wien
Ayrat Khalimov	TU Clausthal
Tim King	AWS
Sascha Klüppelholz	TU Dresden
Konstantin Kueffner	IST Austria
Jan Křetínský	Masaryk University
Ondřej Lengál	Brno University of Technology
Stefan Leue	University of Konstanz
Jianwen Li	East China Normal University
Jyun-Ao Lin	National Taipei University of Technology
Andreas Löow	Imperial College London
Benedikt Maderbacher	CISPA Helmholtz Center for Information Security
Enrico Magnago	Amazon Web Services
Kaushik Mallik	IMDEA Software Institute
Assaf Marron	Weizmann Institute of Science
Luca Marzari	TU Wien
Kuldeep S. Meel	Georgia Tech
Baoluo Meng	GE Aerospace Research
Sayan Mitra	University of Illinois at Urbana-Champaign
Sergio Mover	Ecole Polytechnique
Magnus O. Myreen	Chalmers University of Technology
Alexander Nadel	Technion & Nvidia
Nina Narodytska	VMware Research by Broadcom
Aina Niemetz	Stanford University
Julian Parsert	University of Oxford
Corina Pasareanu	CMU, NASA, KBR
Andreas Pavlogiannis	Aarhus University
Tatjana Petrov	University of Konstanz
Pavithra Prabhakar	The University of New Mexico
Mathias Preiner	Stanford University
Stefan Ratschan	Institute of Computer Science, Czech Academy of Sciences
Adrian Rebola Pardo	TU Wien, Johannes Kepler Universität Linz
Giles Reger	Amazon Web Services and The University of Manchester
Sabine Rieder	Technical University of Munich
Kristin Yvonne Rozier	Iowa State University
David Sanan	Singapore Institute of Technology

Mark Santolucito	Barnard College
Christoph Scholl	University of Freiburg
Martina Seidl	Johannes Kepler University Linz
Natasha Sharygina	University of Lugano, Switzerland
Carsten Sinz	Karlsruhe University of Applied Sciences
Fu Song	Chinese Academy of Sciences, China
Mate Soos	Ethereum Foundation
Daniel Stan	LRE EPITA, ICube, University of Strasbourg, France
Christoph Stickel	The MathWorks
Martin Tappler	TU Wien
Tachio Terauchi	Waseda University
Andrea Turrini	Institute of Software, Chinese Academy of Sciences
Yakir Vizel	The Technion
Tomas Vojnar	Masaryk University and Brno University of Technology
Georg Weissenbacher	TU Wien
Michael Whalen	AWS
Anton Wijs	Eindhoven University of Technology
Tichakorn Wongpiromsarn	Iowa State University
Haoze Wu	Amherst College
Bai Xue	Chinese Academy of Sciences
Emily Yu	Leiden University
Hongce Zhang	Hong Kong University of Science and Technology (Guangzhou)
Zhen Zhang	Utah State University
Yoni Zohar	Bar-Ilan University

FMCAD 2026 Student Forum Committee

Tanja Schindler (co-chair)	University of Basel
Lee Barnett (co-chair)	Amazon Web Services
Haniel Barbosa	Universidade Federal de Minas Gerais
Martin Blicha	University of Lugano
Roderick Bloem	Graz University of Technology
Julie Cailler	University of Lorraine, CNRS, Inria, LORIA, Nancy, France
Constantin Enea	Ecole Polytechnique
Katalin Fazekas	TU Wien
Marijn Heule	Carnegie Mellon University
Marie-Christine Jakobs	Ludwig-Maximilians-Universität München
Mikoláš Janota	Czech Technical University in Prague
Katherine Kosaian	University of Iowa
Kasper Luckow	Amazon Web Services
Nina Narodytska	VMware Research by Broadcom
Michael Rawson	University of Southampton
Kristin Yvonne Rozier	Iowa State University
Martina Seidl	Johannes Kepler University Linz
Jan Strejček	Masaryk University
Martin Suda	Czech Technical University in Prague

Cesare Tinelli
Ashish Tiwari
Nestan Tsiskaridze
Emily Yu
Hongce Zhang
Shufang Zhu
Yoni Zohar

The University of Iowa
Microsoft
Stanford University
Leiden University
Hong Kong University of Science and Technology (Guangzhou)
University of Liverpool
Bar-Ilan University

Additional Reviewers

Agarwal, Chaitanya
Agarwal, Tripti
Ashraf, Sobia
Aurandt, Alexis
Azeem, Muqsit

Baier, Daniel
Becchi, Anna
Becker-Kupczok, Jonas
Benerecetti, Massimo
Berger, Zvika
Berthon, Raphaël
Beutner, Raven
Bhatti, Iram Tariq
Boetius, David
Bork, Alexander
Bovy, Eline
Braipson, Thomas
Britikov, Konstantin
Burgstaller, Tamim

Cauteruccio, Francesco
Chakraborty, Debraj
Chalupa, Marek
Chen, Hanna
Chen, Xiangdong
Chocholatý, David
Coutelier, Robin

Dacík, Tomáš
Dasgupta, Pallab
Davis, Mason
del Rio Almanjaro, Tereso
Dong, Yanni
Dorfhuber, Florian

England, Matthew

Falah, Amin
Farimani, Hassan
Fiedor, Jan
Fleury, Mathias

Gaba, Pranshu
Gangamreddypalli, Namratha
Ganguly, Deep Kumar
Giles, Noah
Govind, R
Grobelna, Marta
Guha, Shibashis
Gürtler, Tobias

Hader, Thomas
Hamel-de Le Court, Edwin
Hamza, Ameer
Havlena, Vojtěch
He, Shaobo
Hekal, Abdelrahman
Hečko, Michal
Hu, Bingqing

Isac, Omri

Jacobs, Swen
Jain, Himanshu
Jankola, Marek
Johannsen, Chris

Kern, Philipp
Kim, Hyondeuk
Kinska, Tereza
Kobus Conrado, Giovanna
Kocourek, Tomáš
Kolárik, Tomáš
Kumar, Ankit
Käfer, Nikolai

Labbaf, Faezeh
Ladner, Tobias
Lal, Ratan
Le, Dylan
Lehmann, Johannes
Leopardi, Fabrizio
Li, Yongjian
Lindner, Andreas
Lingsch-Rosenfeld, Marian
Linker, Felix

Majumdar, Anirban
Malík, Viktor
Manino, Edoardo
Mascherbauer, Dominik
Massoud, Rehab
McKeown, John
Mehta, Vaibhav
Micheletti, Christian
Moeldrup, Lasse
Mogavero, Fabio
Motwani, Harshit Jitendra
Mukherjee, Sayan
Mukhopadhyay, Diganta

Nagashima, Yutaka
Nalbach, Jasper
Neustroev, Grigory
Nicoletti, Daniele
Noetzli, Andres

Onderka, Jan
Osama, Muhammad

P, Habeeb
Pai, Abhishek
Pal, Abhinandan
Peyrer, Cynthia
Phalakarn, Kittiphon
Pluska, Alexander
Pollitt, Florian
Powers, Hannah
Promies, Valentin

Rao, Shrisha
Rashid, Adnan
Redondi, Gianluca
Reeves, Joseph
Reghem, Gaspard
Reichl, Franz-Xaver
Rogalewicz, Adam

Sadhukhan, Suman
Schidler, André
Schnitzer, Yannik
Schreiber, Dominik
Schäfers, Miriam
Sedláček, Jindřich
Shalmon, Yogev
Shen, Yaxin
Sindoni, Giulia
Spork, Timm
Srivastava, Piyush
Stevanovic, Filip
Stierand, Ingo
Strobel, Jannick
Síč, Juraj

Tasche, Philip
Taylor, Landon
Toledo, Guilherme

van der Wal, Laurens
Varanasi, Sarat Chandra
Visconti, Ivan

Waite, Thomas
Wang, Keyin

Yuceel, Ege

Zingoni, Andrea

Štěpková, Adéla

Table of Contents

Tutorials

Verifying Rust Code with Verus	1
<i>Travis Hance</i>	

Invited Talks

CSLib: Building a Platform for AI-assisted Formal Verification in Lean	2
<i>Clark Barrett</i>	
The Parable of the Square-Dancing Witches and Wizards	3
<i>Claire Xenia Wolf</i>	
The Vampire Diary	4
<i>Laura Kovács</i>	

Student Forum

The FMCAD 2026 Student Forum	5
<i>Tanja Schindler and Lee Barnett</i>	

SAT and MAX-SAT Solving

Verified Real-time Proof Checking for Large-Scale SAT Solving	7
<i>Yong Kiam Tan, Dominik Schreiber, Johannes Åman Pohjola, and Magnus O. Myreen</i>	
Weight-Aware Transformations for MaxSAT	16
<i>Jesse Looney, Nikolaj Bjørner, Haoze Wu, and Nina Narodytska</i>	
Aperture: an Anytime, Complete and Incremental MaxSAT Solver	29
<i>Alexander Nadel, Yam Slonimski, and Ofer Strichman</i>	
Understanding CDCL Solvers via Scalability Studies and Proofdoors	37
<i>Shimin Zhang, Yechuan Xia, Chunxiao Li, Jianwen Li, Moshe Y. Vardi, and Vijay Ganesh</i>	
NobleCount: Revisiting a Forgotten Data Structure for Local Search in SAT	50
<i>Yogev Shalmon, Alexander Nadel, and Ofer Strichman</i>	
SATDiv: An Effective Solver for Diverse SAT Problem	56
<i>Shuangyu Lyu, Chuan Luo, Ruizhi Shi, Yuechen Duan and Chunming Hu</i>	

Decision Procedures for Arithmetic Constraints

MCSAT Modulo Transcendental Arithmetics	63
<i>Jorge Gallego-Hernández, Enrico Lipparini, and Alessio Mansutti</i>	
Solving LIA* Constraints Using Hilbert Bases	74
<i>Mudathir Mohamed, Andrew Reynolds, Cesare Tinelli, and Clark Barrett</i>	

Randomized Satisfiability Checking for Non-Linear Arithmetic over Finite Fields	84
<i>Amir Kafshdar Goharshady, Thomas Hader, Laura Kovács, and Harshit Jitendra Motwani</i>	
F-QLPs over unit relative constraints	94
<i>Piotr Wojciechowski and K. Subramani</i>	
Proofs and Proof Generation	
DSLean: A Framework for Type-Correct Interoperability Between Lean 4 and External DSLs	103
<i>Tate Rowney, Riyaz Ahuja, Jeremy Avigad, and Sean Welleck</i>	
Proof Production for Satisfiability Modulo Finite Fields with Proof Checking in Pacheck and Lean .	113
<i>Pedro Saccomani, Abdalrhman Mohamed, Elizaveta Pertseva, Daniela Kaufmann, Cesare Tinelli, Clark Barrett, and Haniel Barbosa</i>	
Certifying Optimal MEV Strategies with Lean	124
<i>Massimo Bartoletti, Riccardo Marchesin, and Roberto Zunino</i>	
IsaAbduct: A Multi-Strategy Abduction Pipeline for Isabelle/HOL	135
<i>Tiago Campos, Sophie Tourret, Jasmin Blanchette, and Haniel Barbosa</i>	
Lean Certified Bitvector Solving without Bitblasting	147
<i>Jan Onderka, Armin Biere, and Mathias Fleury</i>	
Optimising Constant Matrix Multiplication Circuits is NP-complete	155
<i>Nicolai Fiege and Martin Lange</i>	
Parallel and Efficient Solving Strategies	
Parallel SMT Solving via Dynamic Partitioning, Core-Guided Pruning, and Backbone Detection	161
<i>Ilana Shapiro, Sorin Lerner, and Nikolaj Bjørner</i>	
ParaProofa: A Certifying Parallel Cube-and-Conquer QBF-Solving Framework	175
<i>Cynthia Peyrer, Maximilian Heisinger, and Martina Seidl</i>	
Parallel SAT Sweeping on CNFs	182
<i>Niccolò Rigi-Luperti, Armin Biere, and Dominik Schreiber</i>	
Parallelizing Congruence Closure	189
<i>Zachary Kent and Amar Shah</i>	
Beyond Lemma Sharing – Novel Parallelization Strategies for PDR	200
<i>Verner Vlačić</i>	
Runtime Monitoring and Specification Learning	
Multi-Property Temporal Logic Monitoring	210
<i>Arınç Demir and Dogan Ulus</i>	
Shrinking Mission-time LTL Runtime Monitors with Equality Saturation	220
<i>Christopher Johannsen and Kristin Yvonne Rozier</i>	
Learning GR(1) Specifications from Traces	232
<i>Sam Kouteili, William Fishell, Mark Santolucito, and Ruzica Piskac</i>	

Verification for Security and Privacy

SymCert: Verifying SMT-Based Policy Analyses	238
<i>Emina Torlak</i>	
PolyGram: A Certifying Compiler for Network Policies	248
<i>Anoud Alshnakat, Roberto Guanciale, and Mads Dam</i>	
Efficient Enumeration of Cloud Access Permissions	260
<i>Lee A. Barnett, Loris D'Antoni, Amit Goel, Rami Gökhan Kıcı, Tim King, Kasper Luckow, Neha Rungta, and Yasmine Sharoda</i>	
Privacy-Preserving Robust Monitoring of Dense-Time Temporal Logic	271
<i>Charles Koll, Mike Rosulek, and Houssam Abbas</i>	
Checking Information Flow in Cloud-based IoT Access Control Policies	284
<i>Lorenzo Ceragioli, Letterio Galletta, and Edoardo Lunati</i>	

Specifications and Automata

Symbolic Automata for MTL_0^∞ with Super-Dense Semantics	296
<i>Filippo Fantinato, Alessandro Cimatti, and Stefano Tonetta</i>	
On the Hierarchy of Finite-Word Hyperlanguages	309
<i>Hadar Frenkel and Sarai Sheinvald</i>	
Translating LTL to Lasso Automata	321
<i>Rüdiger Ehlers, Nils Hölzner, and Tobias Kühnel</i>	

Program Verification and Synthesis

Tunable Automation in Automated Program Verification	328
<i>Alexander Bai, Chris Hawblitzel, and Andrea Lattuada</i>	
Verifiable Checks for Business Rule Consistency	338
<i>Joseph Tafese, Arie Gurfinkel, Sam Bayless, Nick Feng, and Milad Hooshyar</i>	
Synthesis with Counterexample Guided Observational Equivalence Graphs	349
<i>Guy Frankel, Rudi Schneider, Michel Steuwer, and Elizabeth Polgreen</i>	
An Extension API for the Concurrent Program Verifier Raven	362
<i>Ekanshdeep Gupta and Thomas Wies</i>	
PSoufflé: Scaling Exact Probabilistic Logic Inference for Program Analysis	372
<i>Xuyang Li, Jiahao Xia, Ahmed Adnan, and Jingbo Wang</i>	
Conditional Rewrite Rule Synthesis with E-Graphs and Implication Propagation	379
<i>Andrew Cheung, Chandrakana Nandi and Sorin Lerner</i>	

Model Checking and Symbolic Representation

On the Complexity of Word-Level Model Checking with Arrays	391
<i>Martin Jonáš, Lea Petřivalská, and Jakub Šárník</i>	
CB-VER: A Stable Foundation for Modular Network Control Plane Verification	402
<i>Dexin Zhang, Timothy Alberdingk Thijm, David Walker, and Aarti Gupta</i>	

Certificate-Aware Property-Directed Reachability	414
<i>Arman Ferdowsi and Laura Kovács</i>	
Validated Binary Decompilation Without Tears	426
<i>Alicia Michael, Nicholas Coughlin, Kait Lam, and Kirsten Winter</i>	
Binary Decision Diagrams Unchained	439
<i>Jaehyeok Choi and Andrew Miner</i>	
Hardware Verification	
Semantics, Operations, and Properties of P3109 Floating-Point Representations in Lean	451
<i>Tung-Che Chang, Sehyeok Park, Jay Lim, and Santosh Nagarakatte</i>	
Ordering-Relation Abstraction for Formal Verification of Bubble Errors in CARRY8-Based Tapped Delay Lines	463
<i>Jakovs Ratners, Nikolajs Tihomorskis, and Arturs Aboltins</i>	
Certified Sequential Sweep Without Unrolling	472
<i>Tobias Seufert and Christoph Scholl</i>	
Lemma Pattern Matching for SMT-based Verification of Analog Mixed-Signal Hardware	485
<i>Kunal Sheth and Sara Achour</i>	
Formal Verification of Mixed-Signal Systems Using Real Number Modeling with SMT-based Model Checking	497
<i>Augusto Mafra and Haniel Barbosa</i>	
Software Verification	
Verifying a Memory Allocator for Rust	506
<i>Sinai Kakishita, Akira Hasegawa, Toshiaki Aoki, Ryuta Kambe, and Yuuki Takano</i>	
Formal Verification of a Memory Allocator for Rust Hypervisors: From Verified to Deployable Code with Functional Equivalence Guarantees	516
<i>Jun Liu, Jingxuan Liu, Shenghao Yuan, David Sanan, Kang Chen, Donggang Cao, and Yongwang Zhao</i>	
Prophecy Variables and Invariants in the Move Prover	527
<i>Dao Bo Yang, Arie Gurfinkel, and Richard Trefler</i>	
Formal Verification of Imperative First-Class Functions in Move	537
<i>Wolfgang Grieskamp, Teng Zhang, Vineeth Kashyap, and Jake Silverman</i>	
Multi-Threaded Software Model Checking via Parallel Trace Abstraction Refinement	549
<i>Max Barth and Marie-Christine Jakobs</i>	
Planning and Reinforcement Learning	
Multi-Agent Planning with Spatio-Temporal and Topological Constraints using STL-GO	561
<i>Sheryl Paul, Vidisha Kudalkar, Anand Balakrishnan, Lars Lindemann, Alberto Speranzon, and Jyotirmoy Deshmukh</i>	
Requirement-Based Testing: Enhancing Reinforcement Learning with Game Theory	573
<i>Ocan Sankur, Thierry Jéron, Nicolas Markey, David Mentré, and Reiya Noguchi</i>	

Probabilistic Verification and Games

dtControl 2+ ϵ : Trading Optimality for Explainability in MDPs via Decision Trees	586
<i>Tereza Kinská, Jan Křetínský, Tobias Meggendorfer, Sabine Rieder, and Maximilian Weininger</i>	
Property-driven Causal Abstractions for Markov Decision Processes	599
<i>Jule Schmidt, Maximilian Weininger, Clemens Dubslaff, David Parker, and Nils Jansen</i>	
Conditional Sampling of Symbolic Markov Chains	610
<i>Gera Weiss and Jules Zisser</i>	
Stochastic Boolean Satisfiability for Two-Player Sequential Games under Uncertainty	621
<i>Chi-Kit Ng, Chih-Hsiang Chuang, and Jie-Hong R. Jiang</i>	
The Game Graph Gym	633
<i>Pete Austin, Daniele Dell’Erba, and Patrick Totzke</i>	

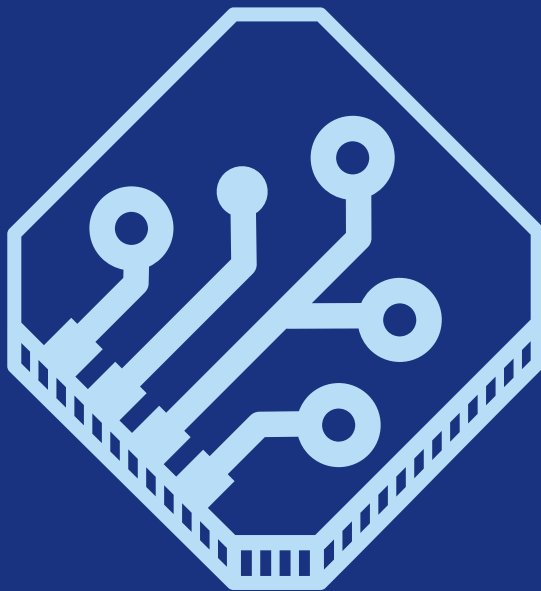
Neural Network Verification

PICID: Proof-Driven Clause Learning in Neural Network Verification	639
<i>Omri Isac, Idan Refaeli, Haoze Wu, Clark Barrett, and Guy Katz</i>	
Incremental Neural Network Verification via Learned Conflicts	652
<i>Raya Elsaleh, Liam Davis, Haoze Wu, and Guy Katz</i>	
Talking with Verifiers: Automatic Specification Generation for Neural Network Verification	665
<i>Yizhak Elboher, Reuven Peleg, Zhouxing Shi, Guy Katz, and Jan Křetínský</i>	
Optimized Piecewise Affine Abstractions of Neural Networks with Learnable Activation Functions .	678
<i>Noah Schwartz, Chandra Kanth Nagesh, Sriram Sankaranarayanan, Ramneet Kaur, Tuhin Sahai, and Susmit Jha</i>	

ML-assisted Reasoning and Verification and Proofs

Can LLMs Perform Synthesis?	694
<i>Derek Egolf, Yuhao Zhou, and Stavros Tripakis</i>	
LLM-Powered Automatic Theorem Proving and Synthesis for Hybrid Systems and Games	707
<i>Aditi Kabra, Jonathan Laurent, Ruben Martins, Stefan Mitsch, and André Platzer</i>	
SVAEval: An Evaluation Framework for LLM-based SVA Property Generators	718
<i>Yu-An Shih, Soohyuk Cho, Aarti Gupta, and Sharad Malik</i>	
Nazrin: An Atomic Neural Proof Automation Tactic in Lean 4	730
<i>Leni Aniva, Iori Oikawa, David Dill, and Clark Barrett</i>	
Trimming Pseudo-Boolean Proofs	743
<i>Berhan Oumer Adame, Bart Bogaerts, Benjamin Bogø, Simon Dold, Arthur Gontier, Wietze Koops, Ciaran McCreesh, Matthew McIlree, Jakob Nordström, Andy Oertel, Adrian Rebola-Pardo, and Mark Turnbull</i>	
Solution Space Partitioning for Extremal Set Theory	757
<i>Jesse Looney, Jonah McDonald, Allison Klingler, Gloria Wu, Jonad Pulaj, and Haoze Wu</i>	

The Conference on Formal Methods in Computer-Aided Design (FMCAD) is an annual conference on the theory and applications of formal methods in hardware and system verification. FMCAD provides a leading forum to researchers in academia and industry for presenting and discussing groundbreaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems. FMCAD covers formal aspects of computer-aided system design including verification, specification, synthesis, and testing.



ISBN 978-3-85448-093-8



9 783854 480938

www.tuwien.at/academicpress